STATEWIDE INFORMATION SYSTEMS POLICY

Statewide Policy: Logging On and Logging Off Computer Resources

Product ID: ENT-SEC-072

Effective Date: October 2004

Approved: Steve Bender, Acting Director, Department of Administration

Replaces & Supercedes: This policy supercedes any prior enterprise policies for establishing and implementing information technology (IT) policies and standards.

I. Authorizations, Roles, & Responsibilities

Pursuant to the Montana Information Technology Act ("MITA") (Title 2, Chapter 17, Part 5 of the Montana Code Annotated ("MCA"), it is the policy of the state that information technology be used to improve the quality of life of Montana citizens, and that such improvement is to be realized by protecting individual privacy and the privacy of the information contained within the state's information technology systems. §2-17-505(1), MCA. It is also the policy of the state that the development of information technology resources be conducted in an organized, deliberative, and cost-effective manner, which necessitates the development of statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and others using the state network. It is also anticipated that State information technology systems will be developed in cooperation with the federal government and local governments with the objective of providing seamless access to information and services to the greatest degree possible. §2-17-505(2), MCA.

Department of Administration: Under MITA, the Department of Administration ("DOA") is responsible for carrying out the planning and program responsibilities for information technology for state government (except the national guard), including for establishing and enforcing a state strategic information technology plan and establishing and enforcing statewide information technology policies and standards. DOA is responsible for implementing MITA and all other laws for the use of information technology in state government. The director of DOA has appointed the chief information officer to assist in carrying out the department's information technology duties. §2-17-512, MCA.

Department Heads: Each department head is responsible for ensuring an adequate level of security for all data within their department. §2-15-114, MCA.

II. Policy - Requirements

A. Scope

This policy applies to all state employees and state contractors using a state computer. This policy does not apply to public access computers.

B. Requirements

State entities must provide for the security of their data and information resources. Access to these resources must be controlled by: users properly logging on and off the network, users not using another employee's UserID, and user's having only one simultaneous connection on the network. Agency Security Contacts should document exceptions to simultaneous connections if they are needed.

All users must be positively identified prior to being able to use any state computer resource. Positive identification involves both a userID and a password which are unique to the individual.

All state computers used by a state employee or state contractor must have a warning banner displayed at all access points. This banner must warn authorized and unauthorized users of the following:

- what is considered the proper use of the system,
- that the system is being monitored to detect improper use and other illicit activity, and
- that there is no expectation of privacy while using the system.

SAMPLE WARNING BANNER

This computer is the property of the State of Montana and subject to the appropriate use policies located at: http://itsd.mt.gov/policy/itpolicy.asp. Unauthorized use is a violation of 45-6-311, MCA. This computer system, including all related equipment, networks, and network devices, is provided only for authorized state government use. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized personnel. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use. **Log off immediately** if you do not agree to the conditions stated in this warning.

Users leaving their computers unattended for 15 minutes or longer must either log off the network or have the screen protected with a password.

C. Background - History On The Creation Of Or Changes To This Policy

This policy was created by the NetWare Managers Group Policy Committee. It was updated in September, 2000 by the State Information Security Manager. This policy was then updated in March, 2004 by the State Security Committee.

D. Guidelines - Recommendations, Not Requirements

When users leave work at the end of each day they must logoff the network and power off their workstation(s). Exceptions to this guideline include workstations that must be left on to run nighttime jobs. In these cases, the monitor must have a password protected screen saver to prevent unauthorized access.

All agency resources should be released (logged off) when not in use.

All entities that use the state's network that are not included within the scope of this policy are encouraged to adopt a similar policy.

E. Change Control and Exceptions

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this policy are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

III. Close

For questions or comments about this instrument, contact the Information Technology Services Division at ITSD Service Desk, or:

Chief Information Officer
PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

IV. Cross-Reference Guide

A. State/Federal Laws

- 2-17-505(1) – Policy
- 2-17-514(1) – Enforcement
- §2-17-505(2), MCA
- §2-17-512, MCA
- §2-15-114, MCA
- 2-17-503, MCA
- 2-15-114, MCA
- 45-6-311, MCA

B. State Policies (IT Policies, MOM Policies, ARM Policies)

- 2-15-112, MCA
- ARM 2.13.101 - 2.13.107 - Regulation of Communication Facilities
- 1-0250.00, MOM, 01/96
- MOM 3-0130 Discipline
- ARM 2.12.206 Establishing Policies, Standards, Procedures and Guidelines.

C. IT Procedures or Guidelines Supporting this Policy

- Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

V. Administrative Use

Product ID:	ENT-SEC-072
Proponent:	Steve Bender, Acting Director, Department of Administration
Version:	1.1
Approved Date:	July 15, 2008
Effective Date:	October 2004
Change & Review Contact:	ITSD Service Desk
Review Criteria:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	July 1, 2013
Last Review/Revision:	Reviewed July 11, 2008. Non-material changes are necessary.
Change Record:	July 11, 2008 – Non-material changes made: - Standardize instrument format and common components. - Changed to reflect next review date.